Anoniem misdaad melden via internet. Technische en juridische risico's

Hoepman, J.H.; Koops, E.J.; Lueks, Wouter

Published in:
Nederlands Juristenblad

Publication date:
2014

Document Version
Early version, also known as pre-print

Anoniem misdaad melden via internet

Technische en juridische risico's

Jaap-Henk Hoepman, Bert-Jaap Koops, Wouter Lueks[1]

Het meldpunt 'Meld Misdaad Anoniem' wordt via de telefoon aangeboden. Maar wie belt er nu nog? Jongeren maken minder melding van misdrijven via het telefonisch meldpunt.[2] Omdat jongere generaties gewend zijn alles via internet te doen, en de drempel voor online melden naar verwachting sowieso lager ligt dan bij telefonisch melden, zou een internetmeldpunt een goede aanvulling kunnen zijn op de huidige dienst.[3] De Minister van Veiligheid en Justitie heeft in dat licht aan de Tweede Kamer een onderzoek toegezegd naar de mogelijkheden van melden via internet, waarbij de kwaliteit van de meldingen zo goed mogelijk geborgd is en de anonimiteit van de melder gegarandeerd blijft.[4] Maar kan anonimiteit op internet wel voldoende worden gegarandeerd? Welke technische en juridische aspecten zijn van invloed op de haalbaarheid van een internetmeldpunt? En moet alles wat online kan, ook online kunnen?

1. Inleiding[5]

De mogelijkheden van het internet roepen vaak de vraag op hoe iets wat van oudsher offline gebeurt, ook online kan worden toegepast, zonder er bij stil te staan of het wel wenselijk is om alles via internet mogelijk te maken. Bovendien worden niet zelden bij het adagium 'wat offline geldt, moet ook online gelden' wezenlijke verschillen tussen offline en online toepassingen over het hoofd gezien.[6] Het lijkt voor de hand te liggen om in het tijdperk waarin telecommunicatieaanbieders adverteren met de leuze 'Wie belt er nu nog?'[7] mensen niet alleen de gelegenheid te geven om misdaad anoniem te melden via de telefoon, maar ook via het internet. Maar de mogelijke laagdrempeligheid van een internetmeldpunt roept vragen op over de wenselijkheid van zo'n meldpunt. De karakteristieken van het internet vergen een gedegen analyse of de anonimiteit bij een internetmeldpunt wel voldoende[8] kan worden gegarandeerd. Dit brengt ons bij de vraagstellingen die centraal staan in dit artikel: in hoeverre is het technisch en juridisch mogelijk om de anonimiteit van melders te garanderen bij meldingen via internet, en wat zijn mogelijke voor- en nadelen van melden via internet voor de rol die anonieme meldingen spelen in de strafvordering en in het maatschappelijk verkeer?

We beantwoorden deze vragen op hoofdlijnen,[9] op basis van literatuuronderzoek, een analyse van verschillende bestaande meldpunten met vergelijkbare functionaliteit (zoals voor klokkenluiders), een interview met Stichting M. die het telefonisch meldpunt beheert, en een expertbijeenkomst met deskundigen die ervaring hebben met (anonieme) publieke meldingen. We beginnen met een korte schets van het telefonische meldpunt en behandelen vervolgens technische en juridische aspecten van een online meldpunt. Vervolgens reflecteren we over de wenselijkheid van een internetmeldpunt, alvorens onze conclusie en aanbevelingen te presenteren.

2. Het telefonisch meldpunt van Stichting M.[10]

De onafhankelijke Stichting M.[11] exploiteert de meldlijn 'Meld Misdaad Anoniem', waar mensen anoniem informatie kunnen geven over misdrijven. Hierbij is de anonimiteit van de melder van hoofdbelang. Naar aanleiding van een anonieme telefonische melding maakt de stichting een schriftelijke melding en stuurt deze door naar afnemers, die verantwoordelijk zijn voor wat er met de melding gebeurt. Deze afnemers zijn naast publieke partijen (zoals KLPD, FIOD en AIVD) ook private partijen, zoals het Verbond van Verzekeraars en de energienetbeheerders. Zo worden bijvoorbeeld meldingen over illegale hennepkwekerijen ook doorgegeven aan de energienetbeheerders. Of een melding ernstig genoeg is om anoniem te doen dan wel af te handelen wordt bepaald door Stichting M. en haar afnemers. De kernwaarde van het meldpunt is haar garantie van anonimiteit. Bij telefonisch binnenkomende meldingen wordt de anonimiteit van zowel de melder als de melding op verschillende manieren gewaarborgd.

Van normale gebruikers kan nauwelijks worden verwacht dat zij Tor correct opzetten en steeds veilig gebruiken

Getrainde telefonisten zorgen ervoor dat het verslag van de melding anoniem is, wat wordt gecontroleerd door een tweede lezer van Stichting M. Verslagen worden, na de beslissing ze al dan niet door te geven aan afnemers, niet bewaard bij de stichting, en er is geen registratie van welke telefonist welke melding heeft aangenomen. In een Instructie Meld Misdaad Anoniem van het College van Procureurs-Generaal (CPG) is vastgelegd dat verkeersgegevens betreffende het meldpunt alleen bij telecomaanbieders worden opgevraagd in situaties van onmiddellijk dreigend levensgevaar, waarbij de gegevens alleen mogen worden gevorderd als de inlichtingen nodig zijn om het desbetreffende leven te redden.[12] Het 0800-nummer van 'Meld Misdaad Anoniem' wordt niet vermeld op de telefoonrekening van de melder.

3. Technische aspecten

Zoals in de inleiding is opgemerkt worden soms wezenlijke verschillen tussen offline en online toepassingen over het hoofd gezien. In deze sectie inventariseren wij deze verschillen door de risico's in kaart te brengen die een internet-gebaseerd meldpunt met zich meebrengt. Aan de hand daarvan schetsen en toetsen we een aantal mogelijke oplossingsrichtingen.

Bij de melder is van belang de apparatuur (computer, smartphone, of vanuit een internetcafé) en hoe deze verbonden is met de systemen van het meldpunt. Een computer die niet onder beheer van de melder is (zoals een computer op het werk of in een internetcafé) maakt bijvoorbeeld het installeren van software lastiger en beperkt de veiligheid van beveiligde verbindingen.[13] Bij het meldpunt is de interne netwerkarchitectuur van belang. We gaan ervan uit dat het meldpunt voor iedere medewerker in twee fysiek gescheiden systemen voorziet: één om met de melder te communiceren (zoals de telefoon in de huidige situatie), de ander om een melding uiteindelijk in te voeren.

3.1. Risico's voor waarborging van anonimiteit

De kwaliteit van een internetmeldpunt hangt onder andere af van de mate waarin anonimiteitsrisico's beperkt kunnen worden. We bespreken kort de risico's die altijd aanwezig zijn en waarmee dus rekening gehouden moet worden. De mate waarin anonimiteit kan worden doorbroken hangt af van de partij die de gegevens poogt te achterhalen. Personen in de directe omgeving van de melder, externe 'hackers' en opsporingsdiensten hebben ieder andere mogelijkheden hiertoe. Een precieze analyse hiervan valt echter buiten de reikwijdte van dit artikel.

3.1.1. Algemeen risico: internetten genereert metadata

De aard van het internet maakt dat metadata (verkeersgegevens over de communicatie), en dan met name informatie over de verzender en ontvanger van een bericht, altijd zichtbaar zijn. Dit is te verhelpen door een anonimiseringssysteem als Tor[14] te gebruiken. Tor verbergt de koppeling tussen verzender en ontvanger zodat niemand kan zien wie er met het meldpunt communiceert. Tor vergt de nodige inspanning van gebruikers; van normale gebruikers kan nauwelijks worden verwacht dat zij Tor correct opzetten en steeds veilig gebruiken.

3.1.2. Risico's bij melder, ISP en meldpunt

Risico's voor anonimiteit bestaan in alle fasen van de communicatie tussen melder en meldpunt (figuur 1).

Aan de kant van de melder ontstaan kwetsbaarheden omdat de melder onzorgvuldig kan zijn en de instructies voor veilig gebruik (bijvoorbeeld over het gebruik van *Private Browsing*[16]) niet goed opvolgt. Daar komt bij dat

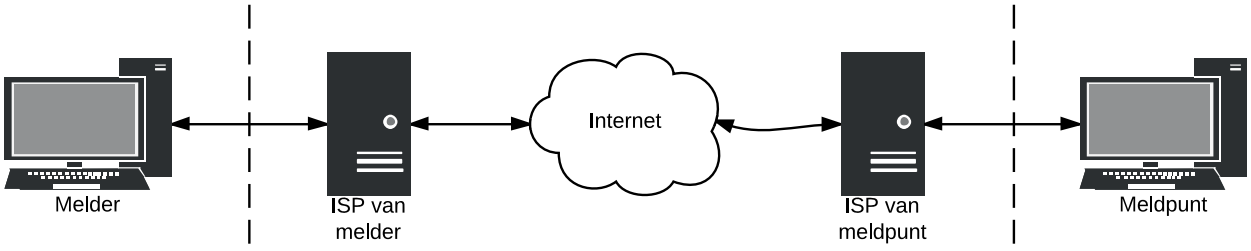
Auteurs

1. Dr. J.H. Hoepman is universitair hoofddocent informatiebeveiliging aan de Radboud Universiteit Nijmegen. Prof. dr. E.J. Koops is hoogleraar regulering van technologie, Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University. Drs. W. Lueks is promovendus informatiebeveiliging aan de Radboud Universiteit Nijmegen. De auteurs zijn tevens verbonden aan het Privacy & Identity Lab (PI.lab).

Noten

2. Interview Stichting M., 7 januari 2014.
3. Vergelijk *Kamerstukken II* 2012/13, 29628, 368, p. 6.
4. *Kamerstukken II* 2012/13, 29628, 400, p. 2.
5. Dit artikel is gebaseerd op een onderzoeksrapport geschreven in opdracht van het WODC: J.-H. Hoepman, B.J. Koops & W. Lueks (2014), *Haalbaarheid van een anoniem misdaadmeldpunt via het Internet. Een quickscan*, Nijmegen/Den Haag: PI.lab/WODC (hierna: rapport), www.wodc.nl/images/2398-volledige-tekst_tcm44-554090.pdf (alle URL's in dit artikel zijn het laatst geraadpleegd op 2 december 2014).
6. M.H.M. Schellekens, 'What Holds Offline, Also Holds On-line?', in: B.J. Koops et al. (eds.), *Starting Points for ICT Regulation. Deconstructing Prevalent Policy One-Liners*, The Hague: T.M.C. Asser Press 2006, p. 51-75.
7. www.youtube.com/watch?v=VhpW4PPhTpk.
8. Anonimiteit is geen zwart/wit-begrip. Absolute anonimiteit zal (vrijwel) onmogelijk zijn, en is als zodanig ook niet nodig voor een werkbaar systeem van anoniem melden. Relevanter is het te kijken of een voldoende mate van anonimiteit bewerkstelligd kan worden.
9. Dit artikel biedt ruimte voor een beknopte bespreking. Voor een uitvoeriger analyse, inclusief organisatorische aspecten, zie ons rapport (noot 5), alsook S. Boes, *M. van A tot Z: een analyse van Stichting M. als voorziening tot burgerparticipatie op het gebied van sociale veiligheid*, Masterscriptie criminologie, Universiteit Leiden 2010 en M. van Kuik e.a., *M.-waarde*, Politie & Wetenschap, 2012.
10. Gegevens zijn ontleend aan het interview (noot 2) en Boes, a.w., noot 9.
11. Stichting M. heet sinds 1 januari 2014 NL Confidential. Omdat in literatuur en beleidsstukken meestal nog gesproken wordt over Stichting M., hanteren wij voor de duidelijkheid in dit artikel de oude naam.
12. College van Procureurs-Generaal, *Instructie meld misdaad anoniem*, 10 april 2006, registratienummer 2006I007.
13. Een bedrijf had enige tijd beschikking over een certificaat van Trustwave waardoor al het beveiligde verkeer onderschept en afgeluisterd kon worden, zie http://blog.spiderlabs.com/2012/02/clarifying-the-trustwave-ca-policy-update.html.
14. www.torproject.org/.
15. Zie bijv. A.S. Tanenbaum & D.J. Wetherall, *Computer Networks*, Prentice Hall 2011.
16. https://en.wikipedia.org/wiki/Privacy_mode.

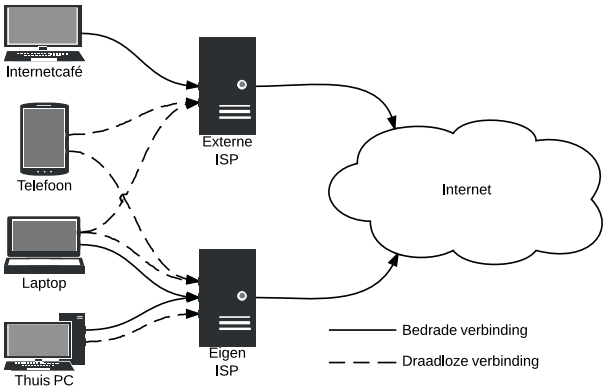
© Ger Loeffen / Hollandse Hoogte



Figuur 1 Communicatie tussen melder en meldpunt.[15]

de sporen die worden achtergelaten niet goed te overzien zijn. Is na het wissen van de browsergeschiedenis deze echt weg of toch nog met forensische hulpmiddelen te achterhalen? Tot slot is het systeem van de melder kwetsbaar; de beveiliging is vaak niet geactualiseerd waardoor derden gemakkelijk toegang kunnen krijgen tot het systeem.

Het verkeer dat de melder verlaat gaat naar zijn ISP. Figuur 2 geeft enkele mogelijkheden weer. Als de melder een onbeveiligd draadloos netwerk gebruikt (en dit is vaak het geval bij openbare netwerken) is dit verkeer eenvoudig af te luisteren of zelfs actief aan te vallen.[17] Daarna stroomt het verkeer via de ISP van de melder over het internet naar de ISP van het meldpunt. Op al deze punten kan communicatie onderschept worden. We schatten dit risico laag in omdat de beveiliging bij deze partijen meestal goed op orde is. Externe ISP's (die niet betaald worden door de melder) bieden echter mogelijk minder garanties of hebben andere belangen. De ISP van het meldpunt is mogelijk een interessanter doelwit is omdat daar alle meldingen langskomen.



Figuur 2. Communicatiekanaal tussen melder en internet. Externe ISP's betreffen een internetcafé of een openbaar hotspot in een trein, café of hotel.

Wanneer meldingen aankomen bij het meldpunt, worden ten behoeve van de communicatie met de melder data tijdelijk opgeslagen. Het is moeilijk te garanderen dat deze daarna nooit te achterhalen zijn. Ook vormen zowel de server waarop meldingen binnenkomen als de terminals waarop meldingen worden weergegeven een risico: deze systemen zijn zowel elektronisch (op afstand) als fysiek (lokaal) kwetsbaar.

3.2. Toetsingscriteria

De anonimiteit kan op twee conceptueel verschillende manieren geschonden worden. Ten eerste kunnen er in de *eindpunten* (bij melder en meldpunt) fouten gemaakt worden waardoor gedurende of na afloop van de melding de anonimiteit in gevaar kan komen. Ten tweede kan de anonimiteit geschonden worden op de *tussenliggende verbinding*. Daarbij maken we onderscheid tussen het lekken van metadata (wie communiceert er met het meldpunt, en vanaf welke locatie) en het lekken van de inhoud van de communicatie. Aangezien de keten zo zwak is als de zwakste schakel, moet de anonimiteit op al deze punten afdoende worden gewaarborgd.

Verder zijn de volgende criteria van belang voor de kwaliteit en effectiviteit van de technische inrichting.

- *De technische eenvoud* van een inrichting bepaalt hoe eenvoudig deze te implementeren is, maar ook hoe eenvoudig de risico's ten aanzien van de anonimiteit in de eindpunten te overzien zijn.
- *Het gebruiksgemak voor de gebruiker* bepaalt mede of een inrichting (goed) wordt gebruikt.
- *De kwaliteit van de melding* is voor het meldpunt een van de belangrijkste criteria. Stichting M. heeft aangegeven dat interactieve communicatie met de melder hiervoor essentieel is. 'De kwaliteit van de melding staat of valt met de mogelijkheid een dialoog te voeren met de melder. In één enkel telefoongesprek zijn de telefonisten in staat om een vertrouwensband met de melder op te bouwen, die hen in staat stelt de serieusheid van de melding in te schatten, en ervoor te zorgen dat de melding voldoende aanknopingspunten voor vervolgstappen bevat.'[18]

3.3. Analyse van mogelijke technische inrichtingen

We schetsen een aantal mogelijke technische inrichtingen en toetsen deze aan de genoemde criteria (zie tabel 1). Omdat consistent gebruik van Tor niet realistisch is, scoren alle inrichtingen met uitzondering van de app slecht op metadata.

1) Een *website* is eenvoudig te gebruiken voor melders, een versleutelde verbinding beschermt de inhoud[19] en een website biedt verschillende mogelijkheden. Een *webgebaseerd formulier*[20] is technisch eenvoudig en hoewel het geen interactie biedt kan het formulier wel gericht informatie uitvragen. De verwachte kwaliteit van de melding is dus redelijk. Een webgebaseerde chatbox[21] biedt wel interactie (en dus een hogere kwaliteit), maar de inrichting is technisch complexer. Een webgebaseerde berichtenbus bestaat al in de vorm van online klokkenluiderssites[22] maar is desalniettemin complex. Van al deze vormen is de chatbox het eenvoudigst te gebruiken.
2) Ook *e-mail* kan worden gebruikt om meldingen te

Tabel 1. Beoordeling van oplossingsrichtingen. Een + betekent dat een inrichting beter is, dat wil zeggen meer anonimiteit biedt, technisch eenvoudig is, een hoog gebruiksgemak kent, of kwalitatief goede meldingen zal opleveren.

	Anonimiteit in de eindpunten	Anonimiteit verbinding (metadata)	Anonimiteit verbinding (inhoud)	Technische eenvoud	Gebruiksgemak gebruiker	Kwaliteit Melding
Website						
Formulier	+/-	-	+	+/-	+/-	+/-
Chatten	+/-	-	+	-	+	+
Berichtenbox	+/-	-	+	-	+/-	-
E-mail	-	-	-	+/-	-	-
Chatten	-	-	-	+/-	-	+
App	+/-	+	+	-	+	+

17. Moxie Marlinspike, *Defeating SSL*, BlackHat DC 2009, www.blackhat.com/presentations/bh-dc-09/Marlinspike/Black-Hat-DC-09-Marlinspike-Defeating-SSL.pdf.

18. Interview, a.w., noot 2.

19. Hierbij wordt gebruik gemaakt van een zogeheten TLS-kanaal, zie T. Dierks & E. Rescorla, 'The Transport Layer Security (TLS) Protocol Version 1.2', RFC5246.

20. Bijv. het TipSoft WebTips platform, zie www.tipsubmit.com/AccMan/uploads/tipsoft.com/TipSoft%20WebTips.pdf.

21. Bijv. www.meldpunt-kinderporno.nl/.

22. Bijv. Securedrop (https://pressfreedomfoundation.org/securedrop) en Globaleaks (https://globaleaks.org/).

doen. Melders zijn hiermee bekend en technisch is dit eenvoudig op te zetten. Er blijven echter makkelijk sporen achter in beide eindpunten.

3) Bestaande *chatinrichtingen* (bijvoorbeeld Google Talk, Skype, IRC, en Jabber) zijn makkelijk in gebruik, maar data zijn soms onversleuteld, met name op externe servers. Daarnaast blijven lokaal eenvoudig sporen achter. De communicatie is interactief, dus de verwachte kwaliteit is hoog.
4) Een mobiele *app*[23] is eenvoudig in gebruik, kan chat functionaliteit bieden, en kan als enige de anonimiteit van de verbinding garanderen. Echter de aanwezigheid van de app verraadt het gebruik, en een dergelijke applicatie is technisch ingewikkeld.

Zowel een webgebaseerde berichtenbus als e-mail kunnen alleen semi-interactief gebruikt worden; het uitwisselen van berichten verloopt niet in *real time*. We verwachten dat daardoor de kwaliteit van de melding laag is. Hoewel e-mail en chat makkelijk te gebruiken zijn, is *veilig* gebruik ervan (met adequate versleuteling) dat niet. Daarom zijn zowel de anonimiteit en gebruiksgemak als slecht beoordeeld.

We kunnen concluderen dat een webgebaseerde chatoplossing of een app het meest aan de eisen voldoet. In beide gevallen geldt echter dat onzorgvuldige gebruikers en de technische complexiteit van het meldpunt nog altijd behoorlijke risico's met zich meebrengen.

4. Juridische aspecten

Bij de juridische aspecten beperken we ons tot de vragen welke juridische mogelijkheden bestaan om anonimiteit te doorbreken, en welke rol anonieme meldingen spelen in het strafproces. Andere juridische aandachtspunten, zoals voldoen aan wetgeving ter bescherming van persoonsgegevens en aansprakelijkheidsrisico's, zijn belangrijk maar grotendeels hetzelfde als bij het bestaande telefonische meldpunt.[24]

Tussen 2005 en 2009 zijn vijf verzoeken ingediend om verkeersgegevens over het meldpunt te mogen vorderen, die alle zijn geweigerd

4.1. Doorbreking van anonimiteit

Aangezien anonimiteit technisch niet absoluut kan worden afgedwongen, is de vraag hoe groot het risico is dat verschillende partijen de anonimiteit van melders kunnen doorbreken gezien hun juridische mogelijkheden daartoe. Voor politie of justitie zijn vier typen opsporingsbevoegdheden van belang om de identiteit van anonieme melders te kunnen achterhalen.

1) *Onderscheppen van telecommunicatie*. Bij het telefonisch meldpunt geldt dat, als iemand onder tap staat, via nummerherkenning technisch wordt voorkomen dat een gesprek met het meldpunt wordt opgenomen,[25] vergelijkbaar met de technische voorziening bij advocatennummers.[26] Een technische inrichting is relatief eenvoudig bij telefoontaps, maar of een dergelijke filtering ook bij internettaps zo kan worden geconfigureerd dat de integriteit niet wordt gecompromitteerd, is een aandachtspunt voor nader onderzoek.
2) *Vorderen van gegevens*. Bij het telefonisch meldpunt mogen verkeersgegevens alleen worden gevorderd in situaties van onmiddellijk dreigend levensgevaar,[27] met toestemming van het College van Procureurs-Generaal na advies van de Centrale Toetsingscommissie.[28] Tussen 2005 en 2009 zijn vijf verzoeken ingediend om verkeersgegevens over het meldpunt te mogen vorderen, die alle zijn geweigerd.[29] Voor een internetmeldpunt kan dezelfde lijn worden gevolgd als bij het telefonisch meldpunt, door de Instructie Meld Misdaad Anoniem en de Aanwijzing opsporingsbevoegdheden uit te breiden met het internetmeldpunt.
3) *Doorzoeking en inbeslagneming*. Hierop heeft de Instructie niet expliciet betrekking, maar naar de geest ervan zou deze ook moeten gelden voor doorzoeking bij het meldpunt. Dat de Instructie ook op dit soort situaties van toepassing wordt, is vooral belangrijk bij een internetmeldpunt omdat daarbij meer sporen achterblijven. Ook bij een doorzoeking of inbeslagneming elders dan bij het meldpunt kan informatie boven water komen over een melding. De Instructie zou in dat licht generiek van toepassing moeten zijn op alle handelingen waarbij de politie gegevens verkrijgt over contact met het meldpunt, ongeacht de precieze bevoegdheid die is uitgeoefend. In alle gevallen is er bij anonimiteitsopheffing immers een afbreukrisico van het anonieme meldpunt als hulpmiddel in de opsporing.[30]
4) *Oproepen van getuigen*. Theoretisch kan de politie een medewerker van het meldpunt oproepen om te getuigen in een strafzaak, waarbij deze geen beroepshalve verschoningsrecht toekomt. Ook hierop zou de Instructie van toepassing moeten zijn, ook bij een internetmeldpunt.

Hoewel vermoedelijk de politie het meeste belang heeft om incidenteel de identiteit van een melder te achterhalen, kunnen ook andere overheidsdiensten een dergelijk belang hebben. Voor bestuursorganen als de Belastingdienst of sociale zekerheidsdiensten, die geen aftapbevoegdheden of verkeersgegevensvorderingsbevoegdheden kennen, is er weinig risico op anonimiteitsdoorbreking. Dat ligt anders bij inlichtingen- en veiligheidsdiensten; voor zover wij weten geldt daarvoor geen soortgelijke instructie als voor politie en justitie. Deze diensten zouden dus, in theorie, al hun bevoegdheden kunnen inzetten om de identiteit van melders te achterhalen. Hoewel de wetenschap dat inlichtingendiensten anonimiteit kunnen doorbreken niet direct verkillend zal werken op de bereidheid van burgers om misdaad te melden, is het risico niet puur theoretisch: als bijvoorbeeld een jongere zijn vriendengroep ziet radicaliseren en plannen hoort van vrienden om naar Syrië te reizen, zou hij uit vrees voor

sociale uitstoting of ergere represailles kunnen afzien van een anonieme melding, indien zijn identiteit via de AIVD achterhaald en bekend zou kunnen raken. Aan dat risico valt weinig te doen.

Waar de politie alleen in acuut levensbedreigende situaties identificerende gegevens van een melder mag vorderen, zullen private partijen dat ook hooguit in levensbedreigende situaties mogen doen. Dergelijke situaties zijn moeilijk voorstelbaar, zodat het juridische risico van anonimiteitsdoorbreking door private partijen verwaarloosbaar is. Belangrijk is wel dat de telecomaanbieder van het meldpunt, die de belangenafweging maakt om al dan niet gebruikersgegevens te verstrekken, doordrongen is van het normatieve kader en het grote belang van anonimiteit van melders. Dit zou met voorlichting, of eventueel contractueel of via een gedragscode, kunnen worden bewerkstelligd.

4.2. Rol van anonieme meldingen

Bestaande vormen om anonimiteit bij aangifte in het strafproces te faciliteren, gaan uit van gedeeltelijke en ophefbare anonimiteit[31] en niet, zoals bij het meldpunt, van zo sterk mogelijke anonimiteit. De schriftelijke verklaring van een anoniem gebleven getuige komt enigszins in de buurt, maar deze kan alleen als (steun)bewijs worden gebruikt indien de verdediging niet te kennen geeft de persoon te willen (doen) ondervragen (art. 344a lid 3 Sv), en zo'n ondervraging is bij anonieme meldpuntmeldingen per definitie niet de bedoeling. Het nut van anoniem (internet)melden moet dan ook alleen worden gezocht in het verkrijgen van start- of sturingsinformatie en niet (ook) in de eventuele bewijswaarde van meldingen. Melders zullen overigens niet altijd beseffen dat hun melding niet als bewijs kan dienen; verwachtingsmanagement bij potentiële melders is daarom een belangrijk aandachtspunt.

Anonieme meldingen mogen worden gebruikt om een opsporingsonderzoek te starten of lopende onderzoeken nader richting te geven. De vraag is vooral of een anonieme melding een redelijke verdenking kan opleveren, wat de drempel is om bepaalde opsporingsbevoegdheden te mogen inzetten. De jurisprudentie eist meestal dat de politie enig aanvullend onderzoek doet om een melding te verifiëren; de eisen hieromtrent kunnen verschillen naar gelang de urgentie of aard van de melding.[32] Brinkhoff concludeert dat 'over het algemeen weinig eisen worden gesteld aan het nadere onderzoek. De redelijke verdenking wordt betrekkelijk snel aangenomen. Als deze lijn zich voortzet, is het denkbaar dat *de facto* een enkele melding bij de M-lijn voldoende is voor de aanname van de redelijke verdenking. Hiermee zou mijns inziens in dit soort zaken sprake zijn van een uitholling van het begrip redelijke verdenking.'[33]

Mocht een internetmeldpunt laagdrempeliger blijken en leiden tot veel meer meldingen, dan zou het gevolg kunnen zijn dat de politie te weinig tijd en capaciteit heeft om nader onderzoek te doen. Het risico bestaat dan dat de tendens die Brinkhoff schetst wordt voorgezet en dat het systeem van het strafrecht, waarbij de redelijke verdenking - gebaseerd op feiten en omstandigheden - een dragende pijler is, onder druk komt te staan. Anderzijds zou het gevolg ook omgekeerd kunnen zijn, wanneer de politie zich genoodzaakt voelt om scherper meldingen te verifiëren met aanvullend materiaal, omdat anders de waarde van anonieme meldingen te sterk verwatert. Ook is denkbaar dat, als de politie vaker en sneller opsporingshandelingen uitvoert op basis van anonieme meldingen, de rechter strakker gaat controleren op anonieme startinformatie en zwaardere eisen gaat stellen aan aanvullende informatie.

Waar de directe effecten van een laagdrempeliger internetmeldpunt op anonieme startinformatie moeilijk in te schatten zijn, moeten in elk geval mogelijke indirecte effecten onder ogen worden gezien van potentieel misbruik. Naast valse meldingen of zwartmakingen door burgers, bestaat ook een klein maar niet verwaarloosbaar risico dat politie (onrechtmatig verkregen) informatie 'witwast' via de anonieme meldlijn. Om misbruik te voorkomen, valt er veel voor te zeggen om een internetmeldpunt niet (substantieel) laagdrempeliger te maken dan het telefonische meldpunt. Technische configuraties met interactie tussen melder en meldpunt, zoals een chatmodaliteit, zijn in dat opzicht te prefereren, omdat die iets hoogdrempeliger zijn en het meldpunt daarbij eerder valse meldingen, zwartmakingen of informatie-witwassen eruit kan filteren.

5. Wenselijkheid van een internetmeldpunt

Hoewel men erkent dat een internetmeldpunt 'meer inhoudt dan even een websiteje bouwen',[34] lijkt de beleidsdiscussie vooral te kijken naar de technisch-organisatorische mogelijkheid, en niet naar de wenselijkheid van een anoniem internetmeldpunt als zodanig. Daarmee wordt miskend dat het internet een eigen dynamiek kent in het maatschappelijk verkeer, die verder gaat dan een invloed op kwantiteit, kwaliteit en identificeerbaarheid van telecommunicatie. Het internet faciliteert en beïnvloedt daarmee de manier waarop communicatie en sociale contacten plaatsvinden. Daarom moeten ook de mogelijke gevolgen van anonieme internetmeldingen voor maatschappelijke processen in bredere zin worden bestudeerd.

Het anoniem melden van misdaad past in een bredere maatschappelijke tendens van anonieme meldingen.[35] Sommigen vinden deze tendens negatief en wijzen op risico's voor de maatschappelijke omgangsvormen, zoals het

23. Bijv. TipSubmit Mobile, zie www. tipsoft.com/TipSubmitMobile.pdf, maar deze app is niet heel anoniem.

24. Zie verder Rapport, a.w. noot 5, hfdst. 5.

25. Stichting NL Confidential. Persoonlijke mededeling, 9 januari 2014.

26. F. Bongers e.a., *Vooronderzoek evaluatie van automatische nummerherkenning geheimhoudergesprekken advocatuur*, Dialogic/WODC 2013.

27. Zie noot 12.

28. Art. 5.1 Aanwijzing opsporingsbevoegdheden, *Stcrt*. 2011, 3240.

29. Boes, a.w., noot 9, p. 36.

30. Vergelijk Instructie, a.w., noot 12.

31. Zie over de Nederlandse regeling W. Dreissen & O. Nauta, *Anonimiteit in het strafproces*, DSP-groep/WODC, Amsterdam, 2012.

32. S. Brinkhoff, 'Anoniem melden startinformatie voor een strafrechtelijk onderzoek?', *NJB* 2008/965, afl. 20, p. 1224.

33. Ibid.

34. *Kamerstukken II* 2012/13, 29628, 368, p. 6.

35. Vergelijk *NRC Handelsblad* 28 februari 2002, 'Nederland klikland', dat begint met de opmerking: 'Nederland kent tientallen kliklijnen'; H. Schnitzler, 'We leven in een "klikspaan boterspaan"-land', *de Volkskrant* 22 februari 2012.

In een klimaat waarin politiële databanken op tamelijk intransparante wijze ook voor andere doeleinden dan opsporing worden ingezet, zouden politiële databanken niet gevoed moeten worden met ongecontroleerde informatie

versterken van onderling wantrouwen,[36] roddel en achterklap,[37] en een afbreukrisico voor integer institutioneel handelen.[38] Buruma wijst, reflecterend op de zaak Lucia de B., op de veranderende omgang met (valse of verkeerde) aangiften in de strafvordering, mede vanwege het feit 'dat in de afgelopen tien jaar een krachtige impuls is gegeven aan het belasteren van medeburgers. Ik denk in de eerste plaats aan het vergemakkelijken van anonieme tips en aangiften'.[39] Hij signaleert ook risico's voor de integriteit van de politie, wanneer agenten 'die met iemand een appeltje te schillen hebben' anonieme tips kunnen gebruiken om, zonder een juridisch adequate aanleiding, een 'bekende' na te trekken in de hoop dat er iets boven water komt.[40]

Anderen benadrukken de positieve kanten van anoniem melden, omdat het juist tot meer veiligheid en vertrouwen van burgers zou leiden[41] en sociale structuren zou versterken.[42] De introductie van Meld Misdaad Anoniem lijkt ook hoofdzakelijk positief te zijn ontvangen door de bevolking en in de media.[43] Aangezien er verschillende perspectieven bestaan op de normatieve waardering van anonieme meldingen, zou eerst een bredere maatschappelijke en politieke discussie moeten worden gevoerd, alvorens een anoniem internetmeldpunt op te richten.

Een ander relevant aandachtspunt voor de beleidsvorming is het verschuiven of geleidelijk uitbreiden van de functionaliteit van het meldpunt. Het oorspronkelijke en hoofddoel van de anonieme meldlijn is opsporing van misdrijven te faciliteren die anders onbekend zouden blijven omdat mensen geen melding bij de politie willen of durven doen. Het doorgeven van anonieme meldingen aan andere overheidsdiensten dan de politie en private partijen (zoals sociale-zekerheidsdiensten, energienetbeheerders en verzekeraars)[44] roept vragen op over 'due process', wanneer de meldingen leiden tot niet-strafvorderlijke beslissingen. Vindt er hoor en wederhoor plaats? Weet de betrokkene dat een beslissing mede is gebaseerd op een anonieme melding? Kan de betrokkene klagen over het gebruik van anonieme startinformatie? Hoewel deze vragen ook gelden voor het telefonische meldpunt, moet bij de beleidsafweging rond een internetmeldpunt zorgvuldig worden overwogen wie de afnemers zijn en hoe de legitimiteit en rechtsbescherming bij niet-opsporingsgerelateerd gebruik van anonieme meldingen gewaarborgd worden.

Verder raakt het strafrechtelijk systeem steeds meer verweven met bestuursrechtelijke en civielrechtelijke beslissingen, zoals gebiedsverboden en uithuisplaatsingen van kinderen. Ook zonder dat een melding leidt tot opsporingshandelingen, kan de opname van anonieme meldingen in politiesystemen consequenties hebben, bijvoorbeeld door vergunningweigering, verzwaard toezicht door de jeugdzorg of het niet krijgen van een baan wegens het ontbreken van een verklaring omtrent het gedrag (VOG).[45] In een klimaat waarin politiële databanken op tamelijk intransparante wijze ook voor andere doeleinden dan opsporing worden ingezet,[46] is het belangrijk om terughoudend te zijn met het voeden van politiële databanken met ongecontroleerde informatie.

Een en ander betekent dat de beleidsvorming voor een anoniem internetmeldpunt niet alleen technisch-organisatorische haalbaarheid moet beoordelen, maar ook moet beargumenteren waarom zo'n meldpunt wenselijk is. De proportionaliteit en subsidiariteit moeten worden aangetoond. Is er feitelijk wel een probleem dat met een internetmeldpunt wordt opgelost, en wat is het probleem dan precies?[47] En als een anoniem internetmeldpunt wenselijk wordt geacht onder beheer van een private partij en met ook private partijen en niet-politiële overheidsdiensten als afnemers, zal nadrukkelijk het publieke belang moeten worden geborgd in contractuele regels, in een wettelijke basis, en vooral in institutionele verankering van publieke waarden als rechtsbescherming, non-discriminatie, privacy en 'due process'. De overheid dient daarbij een strakke regie te voeren.[48]

6. Conclusies

In dit artikel hebben wij de technische en juridische aspecten van een anoniem internetmeldpunt geanalyseerd. Daarnaast hebben wij ook stilgestaan bij de wenselijkheid van een dergelijk meldpunt.

Uit onze analyse blijkt dat een technisch voldoende veilige inrichting van een anoniem internetmeldpunt geen sinecure is en flinke investeringen vergt. Anonimiteit van melders is lastiger te garanderen dan bij een telefonisch meldpunt. Interactiviteit (de mogelijkheid om direct een dialoog met de melder te voeren) is essentieel voor de kwaliteit (en anonimiteit) van de melding. Een smartphone-app of een webgebaseerde chattoepassing voldoet om die reden het beste aan de criteria. Deze kennen echter wel technische beperkingen. Vanwege de hoge complexiteit verwachten wij dat de kosten voor het inrichten van zo'n internetmeldpunt hoog zullen zijn. Nader onderzoek naar een specifieke inrichting van een smartphone-app of webgebaseerde chattoepassing en daaraan verbonden risico's is daarom gewenst.

Vanuit juridisch perspectief is het verschil tussen een internetmeldpunt en een telefonisch meldpunt minder groot. Zolang de Instructie Meld Misdaad Anoniem van het College van Procureurs-Generaal ook van toepassing wordt verklaard op een internetmeldpunt, vormen justitiële bevoegdheden voor anonimiteitsdoorbreking slechts een beperkt risico. Wel kan een laagdrempelig internetmeldpunt tot ongewenste neveneffecten leiden, zoals een hoger risico op misbruik of een verminderde

bruikbaarheid van anonieme meldingen voor de opsporing; ook in dat opzicht zijn interactieve inrichtingen, die minder laagdrempelig zijn, te prefereren.

Verder zijn er gegronde redenen om stil te staan bij de vraag of het anoniem melden van misdaden via internet wel wenselijk is. Niet alles wat technisch mogelijk is, hoeft te worden gerealiseerd alleen omdat het technisch kan. Er wordt verschillend gedacht over de rol van anonieme meldingen in het maatschappelijk verkeer; een bredere maatschappelijke discussie zou daarom moeten voorafgaan aan een eventuele verandering van bestaande mogelijkheden. Verder moet in beleidsvorming onder ogen worden gezien dat de functionaliteit van het meldpunt gaandeweg kan verschuiven of worden uitgebreid - iets wat regelmatig gebeurt met technische voorzieningen. Hoe kan worden voorkomen dat bij gebruik van anonieme meldingen buiten de opsporing van (ernstige) misdrijven de rechtsbescherming van burgers, zoals hoor en wederhoor en aanvechtbaarheid van beslissingen, gewaarborgd blijft? Een brede reflectie hierop is wenselijk, die zou moeten leiden tot een subsidiariteits- en proportionaliteitstoets voor anonieme meldpunten. In een klimaat waarin politiële databanken op tamelijk intransparante wijze ook voor andere doeleinden dan opsporing worden ingezet, zouden politiële databanken niet gevoed moeten worden met ongecontroleerde informatie. Dit pleit voor terughoudendheid bij het verder faciliteren van anonieme meldingen, zeker als een internetmeldpunt laagdrempeliger zou worden dan het huidige telefonische meldpunt.

Helaas betracht de politiek deze terughoudendheid vooralsnog niet. Ondanks de aanzienlijke aarzelingen over de haalbaarheid van een anoniem internetmeldpunt in ons oorspronkelijke rapport[49] wordt voortvarend begonnen met een proefproject waarin 'de technische en organisatorische aspecten van het meldpunt uitgewerkt' worden.[50] De technische risico's voor anonimiteitsdoorbreking verbonden met een anoniem internetmeldpunt zijn onzes inziens dusdanig groot dat men eerst zou moeten onderzoeken of de best haalbare inrichting überhaupt wel een afdoende niveau van anonimiteit kan garanderen en of de kosten daarvan wel opwegen tegen de baten. Tegelijkertijd zou de maatschappelijke en politieke discussie over de wenselijkheid van een anoniem internetmeldpunt veel breder moeten worden gevoerd, in plaats van simpelweg verder te gaan met alles wat online technisch mogelijk is, ook feitelijk te faciliteren. •

36. Schnitzler, ibid.; E. Lissenberg, *Klokkenluiders en verklikkers*, Afscheidsrede Amsterdam (UvA), 15 februari 2008 ('de introductie van meldlijn M. [heeft] niet bijgedragen tot goed burgerschap', p. 9).

37. K. Schuyt pleit tegen anoniem melden van wetenschapsfraude: 'Je geeft op die manier ruimte aan roddel en achterklap en creëert een sfeer van achterdocht en wantrouwen aan de universiteit. Integriteitsklachten kunnen op deze manier misbruikt worden om concurrenten uit te schakelen', *NRC Handelsblad* 8 februari 2014.

38. Lissenberg, a.w. noot 36, p. 17.

39. Y. Buruma, 'Ongemakkelijke lessen van Lucia', *Delikt en Delinkwent* 2010/40, p. 694.

40. Y. Buruma, 'Het recht op vergetelheid. Politiële en justitiële gegevens in een digitale wereld', in: Broeders, Cuijpers en Prins (red.), *De staat van informatie*, Amsterdam: Amsterdam UP 2011, p. 207.

41. Brinkhoff, a.w. noot 32.

42. Boes, a.w. noot 9, p. 25ff.

43. Blauw Research, *Evaluatie pilot Meld Misdaad Anoniem. Eindrapportage*, Rotterdam: Blauw Research 2003, p. 30 en 43.

44. Boes, a.w. noot 9, p. 48-53.

45. Buruma, a.w. noot 40, p. 209; vergelijk ook voorstellen om gemeenten politiegegevens te laten analyseren bij preventief jeugdbeleid ('Steden runnen hun eigen "inlichtingendienst"', *Trouw* 29 januari 2014) en om een VOG te weigeren louter op basis van politiegegevens (*Kamerstukken II* 2013/14, 33750 VI, 99, p. 2). Vergelijk ABRvS 29 januari 2014, ECLI:NL:RVS:2014:205: een VOG kan worden geweigerd op basis van justitiële gegevens over 'strafbare feiten ter zake waarvan een beslissing tot dagvaarding of seponering of een andere beslissing van het openbaar ministerie is genomen.'

46. Vergelijk Buruma, a.w. noot 40.

47. Vergelijk J. Vranken, '"Wij weten wel wat wij doen"', *NJB* 2014/1271, afl. 26, p. 1733.

48. Wetenschappelijke Raad voor het Regeringsbeleid, *Het borgen van publiek belang*, WRR 2000, p. 12.

49. Rapport, a.w., noot 5.

50. *Kamerstukken II* 2013/14, 29628, 460, p. 2.